

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 01

Investigação Criminal Tecnológica

Fundamentos, métodos e aplicações práticas



01

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Investigação Criminal Tecnológica

Fundamentos, métodos e aplicações práticas

*Uma abordagem transversal para investigar fatos, avaliar vestígios e
fundamentar decisões com recursos tecnológicos.*

Coleção Investigação e Proteção na Era Digital
Volume 01

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge

Material educativo de distribuição gratuita.

Coleção Investigação e Proteção na Era Digital, volume 01.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Investigação criminal tecnológica : fundamentos, métodos e aplicações práticas [recurso eletrônico] / Higor Vinicius Nogueira Jorge. -- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (55 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 1)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências e apêndices.

Publicação de distribuição gratuita.

1. Investigação criminal. 2. Tecnologia aplicada à investigação. 3. Vestígios informacionais. 4. Planejamento investigativo. 5. Prova digital. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 A evolução da investigação criminal e a transformação tecnológica.....	7
2 Conceito, objeto e fundamentos da Investigação Criminal Tecnológica.....	10
3 Fundamentos constitucionais e legais da investigação com recursos tecnológicos.....	14
4 Planejamento investigativo, objetivos, hipóteses e estratégias.....	18
5 Fontes de informação e identificação de vestígios relevantes.....	21
6 Técnicas e recursos tecnológicos aplicáveis à investigação.....	24
7 Materialidade, autoria, correlação de dados e limites inferenciais.....	28
8 Diligências tecnológicas: necessidade, proporcionalidade e controle de legalidade.....	31
9 Estudo de caso hipotético com planejamento e desenvolvimento investigativo.....	34
10 Erros frequentes, desafios atuais e perspectivas futuras.....	38
Considerações finais.....	41
Apêndice A. Checklist de planejamento investigativo.....	42
Apêndice B. Matriz de hipóteses investigativas.....	44
Apêndice C. Modelo de linha do tempo.....	46
Apêndice D. Registro de fonte e revisão da conclusão.....	48
Referências.....	50
Minicurrículo do autor.....	52
Para aprofundar o estudo.....	54
A coleção.....	55

Apresentação

Investigar é reconstruir acontecimentos a partir de vestígios, versões e relações que precisam ser demonstradas. A expansão dos meios digitais modificou os lugares em que esses elementos são encontrados e a velocidade com que podem desaparecer. Não eliminou, porém, a necessidade de formular perguntas, confrontar explicações e justificar conclusões.

Um homicídio pode deixar registros em uma câmera; um furto pode ser esclarecido por documentos eletrônicos; uma fraude pode envolver dados bancários, mensagens e depoimentos. A relevância da tecnologia decorre de sua capacidade de apoiar a apuração de crimes de qualquer natureza. Seu emprego exige método, domínio jurídico e compreensão dos limites do que foi obtido.

Esta cartilha desenvolve, em formato didático e aplicado, fundamentos do meu livro *Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais*, publicado pela Editora Juspodivm. Preserva seu eixo conceitual: autonomia da disciplina, transversalidade, vestígio informacional juridicamente relevante, método em sete fases e Controle de Viés Investigativo (Jorge, 2027).

Ao longo do volume, o leitor encontrará fundamentos, orientações de planejamento e um caso hipotético desenvolvido em etapas. Os materiais finais permitem aplicar o raciocínio a situações distintas, mantendo visíveis as informações disponíveis, as lacunas e as decisões necessárias.

O recurso tecnológico deve responder a uma questão definida. A associação entre uma conta e um nome não demonstra, por si, quem executou uma conduta. O compromisso é com conhecimento controlável, respeito aos direitos e precisão para declarar o que ainda não se sabe.

Objetivos e público-alvo

O volume dirige-se a Delegados de Polícia, policiais civis, profissionais da investigação criminal, estudantes e pesquisadores. Oferece uma base comum para o diálogo entre a direção jurídica da investigação, as equipes operacionais e a perícia.

Ao concluir a leitura, o leitor deverá ser capaz de delimitar uma pergunta investigativa, distinguir fontes e categorias de dados, planejar diligências proporcionais, reconhecer limites de atribuição e organizar resultados de modo rastreável. O objetivo não é treinar a operação de um produto específico, mas qualificar escolhas que permanecem relevantes quando as ferramentas mudam.

Como utilizar a cartilha

A leitura sequencial apresenta o método e sua aplicação. Para consulta, os capítulos 3 e 8 tratam dos controles jurídicos; os capítulos 4 e 7 concentram planejamento e raciocínio; o capítulo 9 integra esses conteúdos. Os apêndices oferecem instrumentos preenchíveis.

As expressões “proposta”, “roteiro” e “matriz” identificam recursos de organização sugeridos pelo autor. Regras legais são acompanhadas da indicação de sua fonte. As referências técnicas estrangeiras contribuem com conceitos e cautelas, sem criar poderes investigativos no Brasil.

No texto, “evidência” designa um elemento considerado na análise. A expressão não atribui automaticamente a ele admissibilidade processual ou força suficiente para uma conclusão. O regime da prova e o contraditório exigem avaliação própria, conforme o Código de Processo Penal, especialmente os arts. 155 e 157 (Brasil, 1941).

CAPÍTULO 1

A evolução da investigação criminal e a transformação tecnológica

1.1 A mudança dos ambientes de informação

A investigação tradicionalmente relaciona pessoas, lugares, objetos e acontecimentos. A vida conectada acrescenta registros produzidos por sistemas de comunicação, equipamentos e serviços. O fato pode ocorrer em um espaço físico, enquanto parte de seus vestígios permanece em outro município, em um servidor remoto ou em uma conta controlada por terceiro.

Essa distribuição exige observar o percurso da informação. Uma imagem recebida por mensagem pode ter passado por conversão e compressão; uma planilha pode reunir dados de origens diferentes; um registro de acesso pode representar uma rotina automática. O nome do arquivo ou a aparência da tela não explicam, sozinhos, como o elemento foi produzido.

A transformação relevante não consiste apenas em haver mais dados. Há diferenças na duração dos registros, nas condições de acesso e nas possibilidades de interpretação. O livro que fundamenta esta cartilha examina essa camada informacional como razão para reorganizar o raciocínio investigativo, além da aquisição de equipamentos (Jorge, 2027).

Exemplo hipotético. Na apuração de um furto em depósito, a equipe recebe a fotografia de uma tela que mostra um veículo. Em vez de tratar a fotografia como registro completo, identifica a câmera, o responsável pelo sistema e o intervalo pertinente. Documenta o recebimento e busca a preservação da gravação de origem por via juridicamente adequada. A diligência passa de uma imagem isolada para uma fonte contextualizada.

1.2 Continuidade do método e novas exigências

Entrevistar pessoas, examinar locais e conferir documentos continuam sendo atividades relevantes. A informação digital pode orientar uma entrevista, e a entrevista pode indicar a origem de um registro. O avanço metodológico está

em integrar essas contribuições sem conferir superioridade automática a uma fonte por ela parecer mais tecnológica.

Um vídeo pode não registrar o que ocorreu fora de seu enquadramento. Um depoimento pode explicar quem utilizava um equipamento compartilhado. Um registro administrativo pode delimitar uma oportunidade, mas também refletir erro de lançamento. Cada elemento deve ser avaliado pela questão que consegue responder e pelas condições em que foi produzido.

A investigação ganha consistência quando o resultado pode ser reconstruído por outro profissional. Deve ser possível saber qual material foi examinado, como foi obtido, quais operações foram realizadas e onde estão os fundamentos de cada afirmação. A descrição do caminho percorrido permite avaliar erros, reproduzir verificações possíveis e contestar interpretações.

Erro frequente. Reunir capturas de tela em um documento e chamar o conjunto de “análise técnica” não revela critérios de seleção, origem ou completude. A correção é vincular cada item a um identificador, registrar sua proveniência e separar a apresentação visual da interpretação investigativa.

Aplicação prática. Ao receber um novo elemento, registre o que ele aparenta mostrar e o que ainda precisa ser confirmado. Essa divisão simples reduz a tendência de tomar uma representação parcial como retrato integral do acontecimento.

1.3 Uma investigação orientada por perguntas

A escolha de recursos deve decorrer do problema. Antes de pesquisar uma conta, é necessário definir se a questão envolve sua existência, seu controle em determinado momento ou o conteúdo de uma comunicação. Essas perguntas conduzem a fontes e regimes jurídicos diferentes.

Também importa identificar o que faria a equipe abandonar uma explicação. Se a hipótese é que determinado veículo transportou bens subtraídos, quais elementos seriam esperados? Uma imagem compatível ajuda, mas uma gravação contínua que o mostre imobilizado em outro local pode contrariar a hipótese. O planejamento deve reservar espaço para ambos os resultados.

A ausência de dado não equivale automaticamente à ausência do fato. Para que um resultado negativo tenha significado, é preciso saber se a fonte tinha capacidade de registrar o evento, se o período foi corretamente delimitado e se a busca foi suficiente. Uma câmera sem alimentação elétrica não permite concluir que ninguém passou pelo local.

Síntese de aprendizagem. O uso de tecnologia amplia os ambientes em que se procura informação, mas a qualidade da investigação permanece dependente da pergunta, da fonte e da justificação. O cuidado com vestígios começa no reconhecimento de seu potencial interesse, conforme os arts. 158-A e 158-B do CPP (Brasil, 1941).

Exercício de aplicação. Escolha uma ocorrência hipotética de dano a patrimônio. Liste uma pergunta sobre o fato, uma sobre autoria e uma sobre circunstâncias. Para cada pergunta, indique uma fonte possível e uma limitação. O exercício evidencia que a mesma ferramenta pode ser útil para uma pergunta e inadequada para outra.

CAPÍTULO 2

Conceito, objeto e fundamentos da Investigação Criminal Tecnológica

2.1 Uma definição de trabalho

No livro que fundamenta esta cartilha, a Investigação Criminal Tecnológica é concebida como disciplina autônoma, que organiza o emprego metodologicamente controlado da tecnologia na persecução penal. Sua estrutura articula identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação de vestígios informacionais juridicamente relevantes (Jorge, 2027).

Seu objeto material é o vestígio informacional juridicamente relevante. A finalidade é contribuir para reconstruir o fato, suas circunstâncias e a participação individual. A autonomia resulta da articulação entre método, prova, tecnologia e garantias fundamentais. Não se confunde com informatização policial nem com informática forense, e não cria poderes além dos previstos em lei (Jorge, 2027).

Investigar crimes cibernéticos significa concentrar-se em infrações relacionadas ao ambiente digital ou ao emprego de tecnologias. A abordagem tecnológica é transversal: pode contribuir para apurar um roubo, uma morte suspeita, um desaparecimento ou uma infração ambiental. Há interseção entre as duas perspectivas, sem identidade de alcance.

Exemplo hipotético. Na investigação de incêndio, registros de manutenção, imagens externas e documentos de acesso ao imóvel podem apoiar a reconstrução. A definição da causa do fogo pode exigir perícia específica. Os dados digitais integram o conjunto, sem substituir o exame material nem autorizar conclusão técnica fora da competência de quem analisa.

2.2 Informação, vestígio, evidência e prova

O livro distingue dado, informação, conhecimento, inteligência e prova. O dado é o registro bruto; a informação acrescenta contexto; o conhecimento resulta de

tratamento crítico; a inteligência orienta decisões. A aptidão probatória depende de incorporação válida e controle processual. A passagem entre essas categorias exige verificação, e não ocorre pelo simples uso de um sistema (Jorge, 2027).

Vestígio possui definição legal no art. 158-A do CPP. Seu reconhecimento exige preservação (Brasil, 1941). Um elemento pode ser relevante sem demonstrar a conclusão pretendida. Uma mensagem exige verificações de origem, integridade e interlocutores. O vocabulário deve refletir sua função efetiva.

Os elementos informativos da investigação não se confundem, indistintamente, com a prova submetida ao contraditório judicial. O art. 155 do CPP disciplina essa distinção e ressalva provas cautelares, não repetíveis e antecipadas. A cartilha utiliza “prova digital” como expressão de uso jurídico, sem afastar a necessidade de indicar a etapa e o regime em que o elemento foi produzido (Brasil, 1941).

Precisão na redação. “Foi recebido arquivo atribuído à câmera C1” descreve uma aquisição. “Há sequência compatível com a passagem do veículo” expressa uma observação. “O investigado conduzia o veículo” depende de suporte próprio. Misturar as afirmações oculta o salto inferencial.

Orientação prática. Identifique, para cada afirmação relevante, seu suporte e o passo de raciocínio que conecta o suporte à conclusão. Quando esse passo não puder ser explicado, a conclusão precisa ser revista ou receber qualificação expressa.

2.3 Organização das funções e do conhecimento

No inquérito policial, a direção da investigação cabe ao Delegado de Polícia, nos termos da Lei nº 12.830/2013. A requisição de perícias, informações, documentos e dados integra suas atribuições, respeitados os sigilos e os regimes específicos. O indiciamento exige ato fundamentado e análise técnico-jurídica individualizada (Brasil, 2013, art. 2º).

Essa direção articula conhecimentos diferentes. A equipe investiga fontes e circunstâncias; o analista organiza relações e explicita inferências; o perito realiza exames na forma legal e responde às questões técnico-científicas

pertinentes. A distribuição concreta deve observar as competências profissionais e as normas da instituição. Um relatório investigativo não deve assumir a forma de laudo para conferir aparência de certeza a uma interpretação.

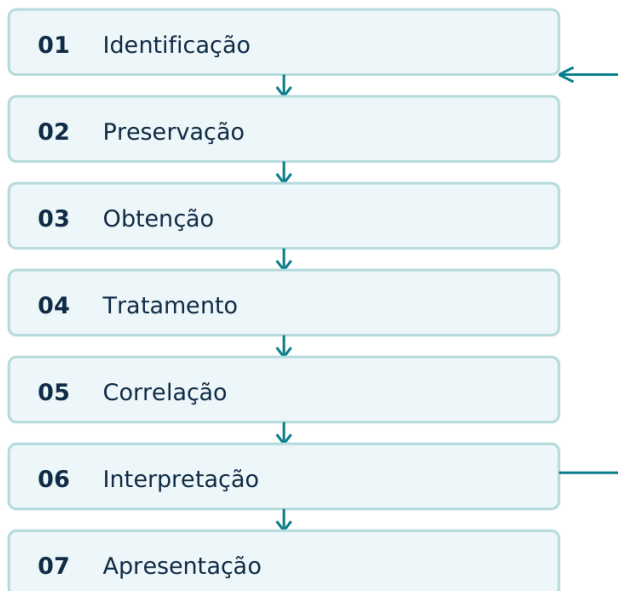
Também não se afirma exclusividade policial sobre toda investigação criminal. A Constituição e o art. 4º, parágrafo único, do CPP permitem reconhecer atribuições de outros órgãos dentro de seus fundamentos próprios. O foco deste volume é o trabalho de polícia judiciária (Brasil, 1988, art. 144; Brasil, 1941).

Síntese de aprendizagem. A abordagem tecnológica combina pergunta relevante, acesso legítimo e análise controlável. A especialização técnica informa a decisão; a decisão jurídica não transforma uma limitação técnica em certeza. A interlocução entre funções deve tornar as fronteiras mais claras.

Pergunta para a equipe. Qual resultado exige exame pericial? Qual depende de diligência externa? Qual demanda decisão do Delegado de Polícia ou autorização judicial? Registrar essas diferenças evita encaminhamentos inadequados e atrasos na preservação de vestígios.

2.4 O método em sete fases

O método desenvolvido no livro estrutura sete fases conectadas. Ele admite retornos: a interpretação pode revelar uma fonte ainda não preservada ou uma obtenção incompleta. Cada retorno exige documentar a nova necessidade e o fundamento da providência (Jorge, 2027).

Figura 1. Método de tratamento do vestígio informacional.

Fonte: síntese didática baseada em Jorge (2027), com representação gráfica própria.

As sete fases organizam a abordagem investigativa. Não substituem as dez etapas da cadeia de custódia previstas no art. 158-B do CPP, que possuem função legal específica (Brasil, 1941). Planejamento, legalidade e documentação atravessam todo o percurso.

CAPÍTULO 3

Fundamentos constitucionais e legais da investigação com recursos tecnológicos

3.1 Direitos fundamentais como critérios de trabalho

A Constituição protege intimidade, vida privada, domicílio, sigilo das comunicações, devido processo e proteção de dados pessoais. Também veda provas ilícitas (Brasil, 1988, art. 5º, X, XI, XII, LIV, LVI e LXXIX). Em coerência com o livro de referência, essas garantias integram a estrutura de legitimidade do método desde o início (Jorge, 2027).

Possibilidade técnica e autorização jurídica respondem a perguntas diferentes. Um aparelho desbloqueado pode permitir operações extensas, mas essa condição não define o alcance legítimo do exame. Uma credencial entregue por terceiro pode funcionar, sem que seu uso esteja juridicamente autorizado. É necessário identificar a fonte de legitimidade do acesso e seus limites.

A competência também precisa ser delimitada. O art. 144 da Constituição distribui funções de segurança pública, enquanto a legislação processual disciplina a apuração e as medidas probatórias. A existência de interesse investigativo não transforma toda base de dados em fonte de livre consulta nem afasta regras de sigilo (Brasil, 1988; Brasil, 1941).

Exemplo hipotético. Ao apreender um computador mediante mandado, a equipe deve conferir o objeto da ordem e documentar sua execução. A apreensão física e o acesso aos dados merecem exame jurídico próprio. A extensão da busca digital precisa ser definida a partir dos fundamentos aplicáveis e da autorização efetivamente existente, sem presumir permissão irrestrita.

3.2 A investigação e o regime da prova

O CPP prevê providências de apuração, preservação do local e coleta de elementos relevantes, além de disciplinar perícia, busca e apreensão. O art. 6º deve ser lido em conjunto com as garantias constitucionais e os dispositivos

específicos de cada medida. A fórmula genérica “interessa à investigação” não resolve restrições de acesso (Brasil, 1941).

Quando a infração deixa vestígios, o art. 158 estabelece a indispensabilidade do exame de corpo de delito, direto ou indireto, não suprido pela confissão. Os arts. 158-A a 158-F organizam a cadeia de custódia. A coleta preferencial por perito oficial, prevista no art. 158-C, reforça a necessidade de articulação com a perícia desde o planejamento (Brasil, 1941).

O art. 157 disciplina a inadmissibilidade da prova ilícita e, em seus termos, das provas dela derivadas. Uma falha técnica de documentação e uma obtenção ilícita não são categorias equivalentes. Cada problema exige identificar a regra violada, a possibilidade de verificação, sua repercussão e o regime processual aplicável. Não cabe oferecer uma solução automática para toda irregularidade.

Orientação prática. Antes de executar a medida, registre: o fato investigado, a finalidade, o fundamento jurídico, quem decide, quem executa e como o resultado será documentado. Quando houver reserva de jurisdição, a iniciativa deve observar a via judicial adequada.

Uma boa justificativa explica o vínculo entre a diligência e o caso. A simples reprodução de artigos, sem demonstrar esse vínculo, não substitui a fundamentação.

3.3 Categorias de dados e sigilos

O Marco Civil da Internet distingue registros de conexão e registros de acesso a aplicações e protege comunicações privadas. Os arts. 7º, 10 e 22 orientam o acesso a registros e conteúdos. A classificação deve preceder o pedido: identificação cadastral, registro de utilização e mensagem privada não são expressões intercambiáveis (Brasil, 2014).

O art. 10, § 3º, preserva, na forma da lei, o acesso por autoridades legalmente competentes a dados cadastrais de qualificação pessoal, filiação e endereço. Essa previsão não transforma histórico de acessos, localização, lista de contatos ou conteúdo de conversa em dado cadastral. O fundamento da requisição precisa ser indicado e o objeto efetivamente limitado.

A preservação cautelar de registros, nos arts. 13 e 15, não equivale à autorização de fornecimento. A medida exige acompanhamento dos prazos legais e dos passos necessários à obtenção judicial. O pedido deve identificar corretamente o objeto para evitar conservar um conjunto inútil ou perder o conjunto pertinente (Brasil, 2014).

A interceptação do fluxo de comunicações obedece à Lei nº 9.296/1996 e depende de ordem judicial, com os requisitos próprios. Sua disciplina não deve ser automaticamente transportada para todo dado já armazenado. Da mesma forma, o fornecimento de dados armazenados não autoriza, por extensão, o monitoramento futuro (Brasil, 1996, arts. 1º a 5º; Brasil, 2014, arts. 7º e 10).

O objetivo deste volume é reconhecer essas fronteiras. Medidas especiais, dados bancários, informações fiscais e cooperação internacional demandam exame de seus regimes próprios.

3.4 Proteção de dados e responsabilidade institucional

A LGPD exclui de sua incidência direta o tratamento para fins exclusivos de segurança pública e de investigação e repressão de infrações penais, nos termos do art. 4º, III. O § 1º do mesmo artigo remete a legislação específica e exige proporcionalidade, estrita necessidade, devido processo, princípios gerais de proteção e direitos do titular. A exclusão não significa liberdade irrestrita de tratamento (Brasil, 2018).

Em termos operacionais, é necessário delimitar quem acessa o material, com qual finalidade e por quanto tempo. Uma pasta compartilhada sem controle pode expor vítimas e testemunhas, além de dificultar a identificação de alterações. O ambiente de análise deve preservar segurança, rastreabilidade e separação entre materiais de diferentes procedimentos.

Dados estranhos ao objeto podem aparecer em exames legítimos. Seu tratamento exige observar o alcance da autorização, o regime jurídico aplicável e decisões da autoridade competente. A equipe deve evitar circulação desnecessária e registrar a situação sem ampliar unilateralmente a medida. A descoberta de nova informação não cria autorização geral para exploração ilimitada.

Síntese de aprendizagem. A legalidade integra o desenho do método. É preciso definir competência, categoria de dado, fundamento, alcance e documentação. O respeito aos direitos fundamentais permite que o conhecimento produzido seja controlado e utilizado dentro de suas condições jurídicas.

Verificação antes da diligência. A equipe consegue explicar qual ato será praticado e por qual fundamento? Se houver dúvida relevante sobre o alcance da autorização, esclareça-a antes do acesso invasivo. A urgência deve ser documentada e encaminhada pela via legal pertinente.

CAPÍTULO 4

Planejamento investigativo, objetivos, hipóteses e estratégias

4.1 Delimitar o problema

Um plano começa pela delimitação do acontecimento, do intervalo temporal e das perguntas ainda abertas. A narrativa inicial pode ser incompleta ou contraditória. Em vez de eliminá-la, essa condição deve aparecer no registro de trabalho: o que foi relatado, o que foi observado e o que depende de verificação.

Perguntas excessivamente amplas, como “descobrir tudo sobre o suspeito”, favorecem dispersão e coleta desnecessária. Uma pergunta operacional, como “quem utilizou o veículo na faixa de horário relacionada ao fato?”, orienta a identificação de fontes e permite avaliar se a diligência cumpriu seu propósito.

A hipótese descreve uma explicação possível para o acontecimento. Deve ser suficientemente clara para produzir consequências verificáveis. “Houve participação de empregado com acesso ao depósito” precisa ser confrontada com a hipótese de uso indevido de credencial e com outras explicações compatíveis com os dados iniciais.

Exemplo hipotético. Após o desaparecimento de equipamentos, há registro de entrada com a credencial de uma funcionária. O plano separa a autenticação do sistema, a presença física e a retirada dos bens. A hipótese de atuação da funcionária não pode excluir, antecipadamente, compartilhamento, clonagem, erro de registro ou acesso de terceiro.

Primeiro registro. Descreva o fato em poucas linhas, enumere as perguntas e identifique os elementos já disponíveis. Uma boa síntese inicial facilita a divisão de tarefas e impede que cada integrante trabalhe com uma versão diferente do problema.

4.2 Hipóteses concorrentes e diligências discriminantes

O Controle de Viés Investigativo (CVI), desenvolvido no livro, exige formular hipótese alternativa plausível, identificar o elemento capaz de sustentá-la e

definir a diligência para testá-la (Jorge, 2027). A matriz desta cartilha operacionaliza esse controle. Não atribui probabilidades numéricas nem substitui a motivação jurídica.

Considere duas explicações: retirada por empregado autorizado ou ingresso de terceiro com credencial emprestada. Uma imagem do portão pode ser mais discriminante do que outra impressão do mesmo registro eletrônico. O planejamento deve buscar informação que acrescente capacidade de distinção, sem repetir indefinidamente a fonte inicial.

Quadro 1. Perguntas que qualificam uma hipótese

Pergunta	Função no planejamento
O que a hipótese explica?	Delimitar sua proposição central.
O que seria esperado se fosse correta?	Orientar verificações concretas.
Que resultado a enfraqueceria?	Prever revisão e evitar confirmação seletiva.
Qual hipótese alternativa permanece?	Preservar explicações concorrentes.
Qual fonte pode distingui-las?	Priorizar diligência com utilidade real.

Fonte: elaboração autoral.

O resultado esperado deve ser definido antes da consulta sempre que possível. Se a expectativa for alterada depois, registre a mudança e seu motivo. Essa transparência permite compreender se a nova interpretação decorreu de evidência adicional ou de adaptação oportunista da narrativa.

Erro frequente. Classificar toda ausência como “conduta de ocultação” torna a hipótese imune a teste. Uma explicação que absorve qualquer resultado sem revisão deixa de orientar uma apuração crítica.

4.3 Prioridade, execução e revisão

A prioridade deve considerar risco às pessoas, volatilidade do vestígio, relevância e viabilidade jurídica. Esses fatores não se reduzem a uma soma automática. Uma fonte importante pode exigir medida judicial; outra, mais

simples, pode desaparecer antes. O Delegado de Polícia coordena a sequência juridicamente cabível com apoio das informações técnicas disponíveis.

O plano deve identificar responsável, prazo, dependências e resultado esperado. “Obter imagens” é insuficiente. “Identificar o responsável pela câmera C1, preservar o intervalo delimitado e documentar a origem do arquivo” permite acompanhar a execução e verificar o que foi efetivamente alcançado.

Resultados negativos também devem ser registrados: fonte indisponível, retenção encerrada, falha na exportação, resposta incompleta. Sem essa documentação, outra equipe pode repetir a tentativa ou interpretar a lacuna como inexistência do fato. A revisão do plano deve considerar o que foi aprendido e o que perdeu utilidade.

Critério de encerramento de uma linha. Uma linha pode ser encerrada quando a pergunta estiver suficientemente esclarecida, quando seu pressuposto for refutado ou quando as diligências adicionais justificáveis não forem capazes de avançar. A razão deve ser registrada. O encerramento de uma linha não transforma uma hipótese concorrente em verdadeira por exclusão incompleta.

Síntese de aprendizagem. Planejar é relacionar perguntas, hipóteses, fontes, autorizações e responsáveis. Revisar o plano faz parte do método. A matriz de hipóteses do Apêndice B ajuda a tornar esse raciocínio visível e a justificar mudanças de direção.

CAPÍTULO 5

Fontes de informação e identificação de vestígios relevantes

5.1 Mapear a fonte antes de interpretar

O mapeamento identifica onde a informação pode existir, quem a administra e como é produzida. Fontes humanas, documentos físicos, equipamentos, sistemas institucionais e serviços de internet podem registrar partes diferentes do mesmo acontecimento. O objetivo é construir um mapa de possibilidades, sem supor que todas serão acessíveis ou confiáveis.

Convém separar a fonte de origem do canal de recebimento. O policial que recebe um vídeo por correio eletrônico conhece o remetente, mas pode desconhecer a câmera, a exportação e as etapas intermediárias. A identificação dessas etapas evita atribuir ao arquivo recebido propriedades que pertenciam apenas ao sistema original.

Para cada fonte, registre período disponível, responsável, formato provável, limitações e medida de preservação ou acesso. A existência de uma política de retenção não garante que os dados concretos foram conservados. A resposta do custodiante e o exame do material devem permitir verificar o alcance real do que foi obtido.

Exemplo hipotético. Um condomínio possui câmeras de acesso e uma plataforma terceirizada para cadastro de visitantes. A câmera pode registrar a imagem, e a plataforma, uma autorização. Nenhum desses elementos, isoladamente, comprova que a pessoa cadastrada foi quem entrou. O plano deve tratar a relação entre ambos como questão a examinar.

Cuidado inicial. Não confunda facilidade de consulta com relevância. Uma fonte pode estar prontamente disponível e contribuir pouco para a pergunta central, enquanto outra exige preservação urgente.

5.2 Fontes abertas e informações entregues

O livro distingue fonte aberta em sentido estrito, conteúdo publicamente acessível, dado comercialmente disponível e medida intrusiva. A acessibilidade técnica não resolve a licitude da origem, do compartilhamento ou do tratamento. A agregação prolongada também exige avaliação de finalidade e proporcionalidade (Jorge, 2027).

Registre endereço, identificadores, data e hora e forma de acesso. A existência pública da página não demonstra a veracidade do conteúdo ou a identidade de quem a controla. Mecanismos de busca são caminhos de localização; seus trechos podem estar incompletos ou desatualizados. Confira a origem e registre o que estava acessível.

Informações entregues por vítima ou testemunha exigem descrição do recebimento. Quem forneceu? Em que suporte? O arquivo foi exportado, encaminhado, convertido ou editado? A obtenção voluntária de um elemento não equivale a permissão ilimitada para examinar a vida digital do entregante ou de terceiros. O âmbito do acesso deve ser juridicamente definido.

Exemplo hipotético. Uma testemunha apresenta captura de anúncio de bem semelhante ao subtraído. A captura orienta a localização da publicação e o exame de características individualizantes. O nome exibido no perfil permanece uma informação a verificar, e a semelhança visual não basta para afirmar que o objeto anunciado é o mesmo.

Erro frequente. Usar consulta aberta como justificativa para ingresso em área restrita, emprego de credencial alheia ou exploração de vulnerabilidade. Essas práticas alteram a natureza da diligência e exigem análise jurídica própria, não resolvida pelo rótulo “fonte aberta”.

5.3 Volatilidade, completude e preservação

A relevância de um vestígio depende de sua relação com a pergunta; a prioridade de preservação também considera o risco de perda. Dados sujeitos a sobrescrita, conteúdo temporário e registros mantidos por prazo limitado pedem providências tempestivas. A urgência precisa ser compatibilizada com a competência e o fundamento da medida.

A preservação deve conservar também contexto suficiente. Um vídeo curto pode omitir a chegada e a saída; uma mensagem recortada pode alterar a compreensão do diálogo. O intervalo adequado não é necessariamente o maior possível, mas aquele justificado pela questão e pelos limites jurídicos aplicáveis.

A cadeia de custódia exige rastrear a história do vestígio. Registros de identificação, recebimento, guarda e movimentação devem acompanhar o material, inclusive quando cópias são produzidas para trabalho. Os arts. 158-A a 158-F do CPP constituem a referência legal dessa organização (Brasil, 1941).

Quadro 2. Resultado negativo e sua interpretação

Situação	Conclusão permitida
Não houve registro e o sistema estava inoperante.	A fonte não permite avaliar o evento.
A busca usou período ou fuso incorreto.	O resultado precisa ser reexaminado.
O registro esperado existe, mas não foi fornecido.	Há lacuna de obtenção.
Fonte apta e consulta adequada não mostram o evento.	A ausência pode ser relevante, com os limites descritos.

Fonte: elaboração autoral.

Síntese de aprendizagem. Uma fonte útil tem origem compreendida, alcance definido e relação demonstrável com o problema. Preservar sua história e suas limitações é parte do trabalho investigativo.

CAPÍTULO 6

Técnicas e recursos tecnológicos aplicáveis à investigação

6.1 Selecionar recursos pela função

Uma técnica deve ser escolhida pelo resultado que pode produzir, pelo material disponível e por seus limites. Pesquisa em fontes abertas, análise de documentos, exame de imagens e correlação temporal respondem a perguntas distintas. A seleção adequada começa por descrever a tarefa em linguagem independente de marcas.

O livro de referência situa esses recursos dentro do método, articulando informática forense, análise criminal e fundamentos jurídicos. A cartilha acompanha essa perspectiva: localizar uma informação, preservá-la e interpretá-la são operações relacionadas, mas cada uma demanda controles próprios (Jorge, 2027).

Na pesquisa aberta, delimite identificadores, termos e intervalo. Na análise documental, estabeleça critérios de seleção e registre quais documentos ficaram fora do exame. Na análise de imagens, diferencie o que é visível daquilo que é apenas compatível com a resolução disponível. Melhorias de contraste ou ampliação devem ser documentadas e não podem inventar detalhes ausentes.

Exemplo hipotético. Uma placa parcialmente legível pode orientar a busca de veículos com características compatíveis. Não autoriza apresentar como leitura certa os caracteres reconstruídos por expectativa. A conclusão deve declarar a parte observada e a parte não resolvida, preservando a imagem recebida e as versões de trabalho.

Orientação prática. Antes de empregar um recurso, responda: qual pergunta ele atende, qual entrada utiliza, que saída produz e como será conferida? A falta de resposta impede avaliar sua utilidade e seu risco de erro.

6.2 Organização, tratamento e documentação

O tratamento converte o acervo em material examinável sem apagar sua proveniência. Um inventário deve associar identificador, descrição, fonte, data de recebimento, localização e restrições. A nomenclatura pode ser simples, desde que estável e não dependente da memória de quem criou a pasta.

O original recebido deve ser preservado conforme sua natureza e o protocolo aplicável. Conversões, transcrições e extrações destinadas à análise devem ser identificadas como derivados. Uma tabela normalizada não pode substituir silenciosamente a resposta do provedor da qual foi extraída. É necessário conservar a relação entre cada linha e o material de origem.

Na orientação do NIST para resposta a incidentes, coleta, exame, análise e relato são atividades diferenciadas. A contribuição dessa referência é organizacional; não constitui autorização de diligência nem substitui o regime brasileiro de prova (Kent et al., 2006).

Funções hash apoiam a comparação de integridade de objetos digitais delimitados. A documentação deve identificar algoritmo, valor, objeto e momento do cálculo. A verificação demonstra correspondência com a referência registrada, dentro das propriedades do método, sem resolver por si a origem anterior, a autoria ou a veracidade do conteúdo. Em conformidade com o livro, o hash integra um conjunto de controles e registros (Jorge, 2027).

Erro frequente. Confundir duas exportações diferentes com adulteração do mesmo objeto. Antes da comparação, identifique se ambas contêm exatamente o mesmo conjunto de bytes. Um vídeo convertido ou um relatório reexportado pode gerar outro hash sem que isso, isoladamente, demonstre fraude.

6.3 Dispositivos e interface com a perícia

A atuação inicial deve evitar intervenções improvisadas. Registre, de modo seguro e conforme o protocolo, as condições observáveis do equipamento e o contexto em que foi encontrado. Comunique à perícia o estado de alimentação, bloqueio e conectividade, quando verificável sem manipulação indevida, e as ações já realizadas.

Não há comando universal de ligar, desligar ou ativar modo avião. As alternativas envolvem riscos diferentes, como perda de dados voláteis, bloqueio, alteração de registros e comunicação remota. A decisão técnica deve considerar o dispositivo e o protocolo institucional. A referência do NIST sobre dispositivos móveis descreve essas limitações e a necessidade de preservação especializada; seus detalhes operacionais devem ser confrontados com a tecnologia efetivamente examinada (Ayers; Brothers; Jansen, 2014).

O livro atribui especial importância ao primeiro respondedor: sua função é reconhecer e preservar, evitando que o exame futuro seja prejudicado. Essa orientação não o transforma em perito, nem autoriza navegação exploratória no equipamento (Jorge, 2027; Brasil, 1941, arts. 158-A a 158-C).

Quesitos úteis. Os quesitos devem perguntar o que o exame pode esclarecer: quais arquivos correspondem ao intervalo pertinente, quais metadados estão disponíveis e quais limitações atingem a interpretação. Pedidos como “comprovar a participação do investigado” antecipam a conclusão e confundem exame técnico com juízo jurídico de autoria.

Síntese parcial. A boa articulação com a perícia começa antes da remessa. Inclua o contexto indispensável, o objeto do exame, o fundamento do acesso, as condições de apreensão e os registros de custódia.

6.4 Correlação, visualização e automação

Linhas do tempo mostram sequência e lacunas. Mapas ajudam a examinar relações espaciais. Grafos representam vínculos definidos. A utilidade de cada visual depende da regra que conecta os dados: uma linha pode significar comunicação, cadastro comum ou simples coincidência. A legenda deve explicar essa regra e permitir localizar sua fonte.

A inteligência criminal pode orientar prioridades e indicar caminhos. A investigação precisa produzir e documentar os elementos que sustentam as conclusões do caso concreto. O livro destaca essa diferença funcional para impedir que um produto de orientação seja apresentado como demonstração autossuficiente (Jorge, 2027).

Sistemas automatizados podem apoiar classificação e triagem. O resultado exige confronto com as fontes. Na transcrição, confira trechos relevantes no áudio; na extração de texto, examine ambiguidades de leitura; no agrupamento de registros, confira os critérios de correspondência. A facilidade de produzir uma saída não demonstra sua correção.

No uso de inteligência artificial, mantenha finalidade definida, ambiente institucional autorizado e controle humano. Registre sistema, versão disponível, entradas, instruções e verificações. Não insira material sigiloso em serviço externo sem avaliação institucional e fundamento adequado. Conforme o livro, a saída serve ao apoio analítico e não substitui a evidência, sua formalização ou decisões privativas da autoridade policial (Jorge, 2027).

Síntese de aprendizagem. O recurso adequado reduz uma incerteza identificada e permite conferir o caminho do resultado. Quando a ferramenta não oferece controle suficiente, sua saída deve receber a limitação correspondente e não sustentar conclusões além do que foi demonstrado.

CAPÍTULO 7

Materialidade, autoria, correlação de dados e limites inferenciais

7.1 Separar as proposições

Materialidade, autoria e circunstâncias são questões relacionadas, mas distintas. Demonstrar que houve transferência não identifica automaticamente quem a determinou. Demonstrar acesso a um sistema não esclarece, por si, o propósito do acesso. A investigação precisa individualizar o que cada elemento sustenta.

A Lei nº 12.830/2013 exige análise técnico-jurídica fundamentada para o indiciamento, com indicação de autoria, materialidade e circunstâncias. O CPP define indício a partir de circunstância conhecida e provada que permita inferir outra. Essas referências exigem explicitar tanto o suporte quanto o raciocínio, evitando o uso da palavra “indício” para encobrir conjecturas (Brasil, 2013, art. 2º, § 6º; Brasil, 1941, art. 239).

Quadro 3. Categorias de afirmação

Categoria	Forma de apresentar
Fato documentado	Indicar o registro e aquilo que ele demonstra.
Versão ou alegação	Identificar quem relatou e em quais condições.
Indício	Explicitar a circunstância conhecida e a relação inferida.
Inferência investigativa	Expor o caminho entre os elementos e a proposição.
Hipótese investigativa	Declarar a explicação sujeita a teste.
Conclusão fundamentada	Relacionar conjunto, limites e consequência jurídica.

Fonte: elaboração autoral, com referência ao art. 239 do CPP.

Uma afirmação pode mudar de condição ao longo do trabalho. O relato inicial de horário pode ser confirmado, corrigido ou permanecer incerto. A redação deve acompanhar essa mudança, preservando a história da verificação.

7.2 Identificadores técnicos e atribuição pessoal

Titularidade de linha, conta ou assinatura de acesso descreve uma relação cadastral. Utilização de dispositivo ou execução de uma ação são proposições adicionais. Contas podem ser compartilhadas ou comprometidas; credenciais podem ser utilizadas por outra pessoa. O exame de autoria deve considerar controle, oportunidade, contexto e corroboração.

O endereço IP integra a identificação técnica de uma conexão, sem funcionar como identidade civil de quem agiu. Em compartilhamento de endereços, o relacionamento pode exigir porta de origem, data, hora, fuso e registros complementares. A RFC 6302 recomenda registrar portas e horários precisos, além do IP, para lidar com esse cenário. Sua recomendação técnica não cria dever jurídico de guarda no Brasil (Durand et al., 2011).

A associação a uma área de cobertura de telefonia tampouco equivale a localização pontual da pessoa. É necessário compreender a natureza do registro, a cobertura e as limitações técnicas. Em coerência com o livro, correlação espacial e temporal não deve ser convertida diretamente em presença inequívoca ou cumplicidade (Jorge, 2027).

Exemplo hipotético. Uma conta foi acessada por conexão de uma residência com vários moradores. O resultado pode orientar a investigação sobre quem tinha acesso e sobre a integridade das credenciais. Não permite selecionar o titular da assinatura como autor apenas porque seu nome aparece na resposta cadastral.

Orientação prática. Redija a atribuição por níveis: vínculo com cadastro, vínculo com equipamento, controle no momento e relação com a conduta. Indique quais níveis estão demonstrados e quais permanecem em aberto.

7.3 Corroboração, independência e controle de vies

A concordância entre elementos pode aumentar a consistência de uma explicação quando eles acrescentam informação efetiva. Três relatórios que reproduzem a mesma captura não são três confirmações independentes. É necessário reconstruir a origem comum para evitar multiplicar artificialmente o peso de um único elemento.

O Controle de Viés Investigativo exige examinar explicações alternativas plausíveis e elementos exculpatórios. Não se trata de inventar possibilidades remotas para impedir qualquer conclusão. Trata-se de testar alternativas apoiadas nas condições do caso e registrar por que foram fortalecidas, enfraquecidas ou mantidas abertas (Jorge, 2027).

Uma inconsistência também precisa ser examinada antes de ser descartada. Horário divergente pode decorrer de relógio desajustado, interpretação de fuso ou erro de transcrição. Se houver motivo documentado para corrigir a leitura, preserve o valor original e registre a transformação. Corrigir silenciosamente para que a linha do tempo “encaixe” retira a possibilidade de controle.

Exemplo hipotético. Uma imagem sugere passagem às 20h10, enquanto o controle de acesso registra 20h18. A equipe identifica diferença do relógio da câmera por comparação contemporânea documentada. Para o período do fato, avalia se há base para aplicar o ajuste e qual incerteza permanece. Não transforma uma comparação posterior em garantia de sincronismo histórico.

Síntese de aprendizagem. A conclusão deve resistir à pergunta: qual outra explicação compatível com os dados foi testada? A precisão para reconhecer limites protege a apuração e as pessoas contra a falsa certeza produzida por coincidências ou fontes dependentes.

CAPÍTULO 8

Diligências tecnológicas: necessidade, proporcionalidade e controle de legalidade

8.1 Justificar a intervenção

Uma diligência deve ter objeto definido, utilidade demonstrável e fundamento jurídico. A adequação relaciona o meio ao objetivo. A necessidade examina alternativas menos restritivas com capacidade comparável de esclarecimento. A proporcionalidade em sentido estrito avalia se o ganho esperado justifica a restrição envolvida, dentro das condições legais.

Essa organização acompanha a abordagem do livro, que trata os direitos fundamentais como condições da investigação e considera também os efeitos de agregação de informações. A análise alcança extensão, intensidade e duração do tratamento, e não apenas cada consulta isolada (Jorge, 2027; Brasil, 1988, art. 5º).

Exemplo hipotético. Para verificar a retirada de um bem em intervalo delimitado, pode ser pertinente obter a gravação do acesso correspondente. Solicitar todo o histórico de vida digital das pessoas que frequentam o local exige outra justificação e outro exame de legitimidade. A gravidade do crime não dispensa a demonstração de conexão entre objeto e medida.

Fundamentação concreta. O pedido deve explicar qual lacuna será enfrentada, por que a fonte pode preenchê-la, quais identificadores delimitam a busca e quais cautelas reduzirão a exposição de terceiros. Expressões como “para completo esclarecimento” devem ser desenvolvidas em razões relacionadas ao fato.

A avaliação jurídica deve preceder o ato. Uma justificativa construída depois da obtenção não transforma, retrospectivamente, uma intervenção ilegítima em diligência regular.

8.2 Preservar, obter e examinar

Esses verbos descrevem atos diferentes. Preservar visa evitar perda ou alteração. Obter significa receber ou adquirir o material pela via legal. Examinar envolve acessar e processar seu conteúdo dentro do alcance permitido. A autorização de um ato não deve ser ampliada por conveniência operacional.

O Marco Civil permite requerimentos cautelares de guarda de registros e estabelece condições para o acesso judicial. Nos arts. 13, §§ 2º a 5º, e 15, §§ 2º e 3º, a preservação exige acompanhamento do pedido judicial de acesso e dos prazos correspondentes. A guarda cautelar não entrega os registros à autoridade requerente (Brasil, 2014).

Quadro 4. Atos e controles

Ato	Questão a resolver
Consulta pública	O acesso e o tratamento são legítimos e pertinentes?
Requisição cadastral	Há competência legal e objeto cadastral delimitado?
Preservação de registros	Qual fonte, intervalo, fundamento e prazo de acompanhamento?
Fornecimento de registros protegidos	A ordem judicial alcança o conjunto solicitado?
Acesso a comunicações privadas	Qual regime, fundamento e alcance autorizam a medida?
Exame de dispositivo	O acesso está legitimado e o método documentado?

Fonte: elaboração autoral, com base em Brasil (1988, 1941, 1996, 2013, 2014).

As hipóteses especiais devem ser examinadas conforme seus próprios requisitos. Não se presume que uma situação rotulada como urgente autorize fornecimento, monitoramento ou acesso sem o fundamento legal correspondente.

8.3 Execução controlada e prestação de contas

A equipe deve conhecer o alcance da decisão e os limites operacionais antes de executá-la. Identificadores, intervalos, categorias de dados e condições de guarda precisam ser compreendidos por quem fará a solicitação, o recebimento e o exame. Uma ordem corretamente fundamentada ainda pode ser executada de modo excessivo ou tecnicamente inadequado.

No recebimento, confira se a resposta corresponde ao objeto autorizado. Documente arquivos, formatos, período abrangido e lacunas declaradas pelo fornecedor. Respostas negativas ou parciais devem ser tratadas como resultados específicos, sem completar por imaginação o que não foi fornecido.

Se surgir necessidade de ampliar a diligência, registre os novos elementos e submeta a providência à decisão competente. O encontro de dado estranho ao objeto não concede liberdade para explorar todo o acervo. A delimitação protege o exame e permite compreender por que determinada informação passou a integrar a investigação.

O relatório de cumprimento deve identificar o que foi realizado, os responsáveis, os resultados e as ocorrências relevantes. O controle de legalidade não se encerra com a emissão da ordem. Ele abrange execução, tratamento e apresentação, sob as garantias constitucionais e as regras processuais aplicáveis (Brasil, 1988; Brasil, 1941; Jorge, 2027).

Síntese de aprendizagem. A diligência deve poder ser explicada antes, acompanhada durante e reconstruída depois. A fundamentação define a finalidade; os registros mostram se ela foi respeitada. Lacunas e alterações de plano devem permanecer visíveis para quem avaliar o resultado.

CAPÍTULO 9

Estudo de caso hipotético com planejamento e desenvolvimento investigativo

9.1 O problema e as hipóteses

Todo o caso é fictício. Uma empresa comunica a retirada não autorizada de seis equipamentos de seu depósito. A ausência foi percebida na manhã seguinte. O controle eletrônico registra uso da credencial atribuída à funcionária Ana às 20h18. Uma testemunha relata ter visto um veículo utilitário próximo ao portão. Uma imagem encaminhada por mensagem mostra veículo de aparência semelhante.

Esses elementos têm alcances diferentes. A empresa apresenta uma versão sobre a subtração; o registro associa uma credencial a um evento; a testemunha descreve uma percepção; a imagem encaminhada ainda demanda identificação de origem. Não há base para converter automaticamente o nome cadastrado em autoria.

O plano delimita três perguntas: houve retirada indevida dos equipamentos? Quem realizou a retirada? Houve participação de quem controlava ou disponibilizou a credencial? A verificação de inventário, documentos de movimentação e condições do local deve acompanhar a pesquisa de vestígios digitais.

Hipóteses de trabalho. H1: Ana utilizou sua credencial e participou da retirada. H2: terceiro utilizou a credencial, com ou sem conhecimento de Ana. H3: a movimentação foi autorizada ou o controle de estoque contém erro. As hipóteses podem ser refinadas, combinadas ou abandonadas conforme os resultados.

A formulação aplica o Controle de Viés Investigativo: para cada explicação, o plano deve indicar consequência verificável, elemento contrário e diligência discriminante. A análise começa com perguntas, em coerência com o método do livro de referência (Jorge, 2027).

9.2 Identificação, preservação e obtenção

A equipe identifica câmeras do portão e da via próxima, registros administrativos, controle de acesso e pessoas responsáveis pelo estoque. A prioridade de preservação considera a possibilidade de sobrescrita das imagens. O Delegado de Polícia define as providências juridicamente cabíveis, com apoio técnico e articulação pericial.

A imagem recebida é registrada como item E01, com informação sobre remetente, data, canal e limitações de origem. A gravação correspondente é procurada na fonte. Quando legitimamente obtido, o arquivo de origem recebe outro identificador, E02, relacionado a E01. Não se substitui o primeiro item nem se presume identidade entre os dois.

O registro de acesso é individualizado como E03, com documentação sobre exportação, campos e configuração temporal. Os documentos de estoque e movimentação formam E04. O depoimento da testemunha é registrado como E05 e permanece identificado como fonte humana, com o regime processual próprio.

Pedidos de dados protegidos, se necessários, devem indicar fonte, categoria, período e fundamento. A hipótese H2 não autoriza acesso irrestrito às contas de todos os empregados. Preservação e obtenção seguem os regimes legais já examinados (Brasil, 1941; Brasil, 2014).

Controle do escopo. A pergunta sobre quem usou a credencial orienta a busca inicial. A investigação não pressupõe colaboração de Ana nem descarta essa possibilidade. A expectativa de resultado é registrada antes do exame, permitindo avaliar se o material apoia, contraria ou deixa a hipótese sem resposta.

9.3 Tratamento, correlação e interpretação

O exame de E02 revela pessoa com vestimenta distinta daquela atribuída inicialmente a Ana. A resolução não permite identificação facial. O registro mostra o veículo em intervalo compatível com a abertura do portão. E03 contém o identificador da credencial, mas não registra a identidade física de

quem a portava. E04 confirma a ausência dos equipamentos e não revela autorização de saída no período examinado.

Esses resultados enfraquecem uma versão simplificada de H1, mas não demonstram, por si, a inocorrência de participação de Ana. Também não provam H2 integralmente. É necessário investigar controle da credencial, contexto da retirada e eventual participação de outras pessoas, incluindo elementos que possam excluir envolvimento.

Quadro 5. Atualização das hipóteses

Hipótese	Resultado e próximo passo
H1: atuação de Ana	Identificação pessoal não confirmada. Verificar presença e controle da credencial.
H2: uso por terceiro	Compatível com o vídeo. Apurar como ocorreu o acesso e eventual participação de Ana.
H3: movimentação regular ou erro	Documentos examinados não a sustentam. Conferir responsáveis e registros complementares.

Fonte: elaboração autoral. Caso inteiramente hipotético.

A linha do tempo mantém os horários originais e a referência temporal de cada fonte. Diferenças de relógio são registradas como problema a examinar. O diagrama de vínculos, se utilizado, distingue titularidade cadastral de presença e participação. Não se desenha uma relação criminal onde há apenas uma relação administrativa.

9.4 Apresentação e decisão fundamentada

Após novas diligências, uma pessoa afirma ter recebido a credencial para tarefa regular anterior. A informação constitui uma versão a verificar. O reconhecimento do empréstimo, se documentado, não demonstra automaticamente ciência sobre a retirada dos equipamentos. O plano deve testar momento, finalidade, devolução e compatibilidade com outros elementos.

O relatório separa o que foi documentado, o que foi relatado e o que foi inferido. Identifica E01 a E05, as diligências complementares, os resultados negativos e

as limitações. Expõe por que a relação entre a credencial e o cadastro não resolve a atribuição pessoal. A conclusão não é predeterminada pelo roteiro didático.

O indiciamento, se houver suporte, dependerá de análise técnico-jurídica fundamentada do Delegado de Polícia, conforme a Lei nº 12.830/2013. O roteiro não oferece uma quantidade universal de registros capaz de substituir essa análise. Sem elementos suficientes, a insuficiência deve ser declarada e as providências pertinentes avaliadas (Brasil, 2013, art. 2º, § 6º).

Revisão crítica do caso. O método permitiu distinguir conta, credencial, pessoa e conduta. O Controle de Viés Investigativo direcionou a busca de alternativa plausível e impediu que o cadastro encerrasse a apuração. A preservação, a obtenção legítima e a documentação permitiram compreender os limites do conjunto (Jorge, 2027).

Exercício. Redija uma conclusão de cinco linhas sem afirmar quem praticou o fato. Depois, indique a diligência mais útil para reduzir a principal incerteza. A resposta deve justificar a escolha e seu fundamento, sem prometer que o resultado confirmará a hipótese preferida.

CAPÍTULO 10

Erros frequentes, desafios atuais e perspectivas futuras

10.1 Erros que se acumulam

Alguns problemas começam com uma pequena omissão e se ampliam ao longo do trabalho. Um arquivo sem origem clara recebe nome conclusivo; o nome é reproduzido em uma planilha; a planilha alimenta um gráfico; o gráfico aparece no relatório como confirmação. O percurso transforma uma incerteza inicial em aparência de fato por repetição.

A correção exige retornar ao suporte. Identificadores devem ser descritivos, sem antecipar culpa. A categoria “conta consultada” é preferível a “conta do autor” quando a atribuição ainda está aberta. O texto deve deixar clara a diferença entre classificação de trabalho e conclusão sustentada.

Outro erro é acumular material sem pergunta definida. A coleta excessiva amplia exposição de terceiros, aumenta o volume de análise e pode dificultar a localização do que realmente importa. O método do livro exige identificação orientada pela relevância jurídica e controle de escopo desde o primeiro contato com a fonte (Jorge, 2027).

Quadro 6. Erro e correção

Erro	Correção necessária
Titularidade tratada como autoria	Verificar uso, controle e relação com a conduta.
Captura sem origem	Documentar recebimento e buscar contexto verificável.
Fontes repetidas contadas como independentes	Reconstruir sua origem comum.
Ajuste temporal silencioso	Preservar o valor e justificar a transformação.
Resultado automatizado aceito sem conferência	Confrontar a saída com as fontes pertinentes.

Fonte: elaboração autoral.

10.2 Nuvem, falsificações e limites de detecção

A dispersão do material entre dispositivos e serviços exige mapear os locais possíveis de armazenamento. O aparelho pode conter parte do conteúdo, referências a arquivos remotos ou nenhum dos registros desejados. Não há garantia de que o fornecedor conserve o conjunto que a equipe imagina. O livro trata a investigação além do dispositivo e a diferença entre preservar e obter dados como questões estratégicas (Jorge, 2027).

Conteúdos manipulados ou sintéticos reforçam a importância da origem, do contexto e da corroboração independente. Uma aparência convincente não demonstra autenticidade. Ao mesmo tempo, a possibilidade abstrata de manipulação não torna falso todo registro. A resposta é examinar as condições concretas do material, com apoio pericial quando necessário.

Não apresente um detector automático como árbitro infalível. Registre sua função, limitações e a natureza do resultado. A conclusão sobre o arquivo deve considerar o conjunto disponível, sem converter uma pontuação de ferramenta em certeza sobre fabricação ou autenticidade. Essa orientação acompanha a centralidade da proveniência desenvolvida no livro (Jorge, 2027).

Exemplo hipotético. Um áudio atribuído a determinado interlocutor é divulgado em uma rede social. A voz semelhante orienta uma hipótese, mas não resolve origem, edição ou contexto. A equipe busca a fonte, documenta o percurso, confronta outros elementos e avalia exame especializado. Não conclui autenticidade pelo reconhecimento informal nem falsidade pela simples alegação de uso de IA.

10.3 Governança, capacitação e memória institucional

A qualidade não pode depender apenas de um profissional que conhece um programa. A instituição precisa definir quem utiliza os recursos, com quais finalidades, em quais ambientes e com quais registros. A mudança de equipe não deve apagar o conhecimento sobre a origem do material ou o motivo de uma decisão.

A capacitação deve alcançar quem reconhece o vestígio, quem registra sua apreensão, quem armazena, quem analisa e quem decide. O conteúdo varia conforme a função. O primeiro respondedor precisa reconhecer situações de risco e preservar; o analista deve explicar transformações e inferências; a autoridade policial deve fundamentar as providências de sua competência. O livro articula esses deveres como governança permanente (Jorge, 2027).

Uma política de revisão pode incluir conferência por outro integrante, sobretudo em resultados decisivos ou ambíguos. A revisão deve confrontar fonte, método e conclusão, sem se limitar a correções gramaticais. Quando possível, o revisor deve ter espaço para formular explicação alternativa sem pressão para manter a hipótese inicial.

Indicadores úteis são a rastreabilidade dos itens, o cumprimento das providências de preservação, a clareza das limitações e a possibilidade de localizar o suporte das conclusões. A quantidade de arquivos ou gráficos produzidos não mede, sozinha, a qualidade da investigação.

Síntese de aprendizagem. As ferramentas continuarão a mudar. Permanecem relevantes a pergunta, a legalidade, a preservação e o controle do raciocínio. A perspectiva de futuro é institucional: tornar esses cuidados reproduzíveis, compreensíveis e sustentáveis na rotina.

Considerações finais

A Investigação Criminal Tecnológica reúne fundamentos jurídicos, tratamento de vestígios e raciocínio crítico para apurar fatos em uma sociedade informacional. Sua contribuição transversal aparece quando a tecnologia é integrada ao problema investigativo, às fontes humanas e materiais e aos controles de validade.

Esta cartilha desdobra a proposta do livro *Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais em orientações de uso e instrumentos de trabalho*. Preserva o objeto da disciplina, seu método em sete fases e o Controle de Viés Investigativo, com atenção à distinção entre informação que orienta e elemento que sustenta uma conclusão (Jorge, 2027).

O percurso não se encerra com a obtenção de dados. É necessário compreender como foram produzidos, conservar sua história, testar relações e explicar limites. A demonstração de autoria exige individualização e corroboração, sem atribuição automática por cadastro ou coincidência técnica.

A direção jurídica da investigação, o apoio operacional e a perícia devem dialogar a partir de perguntas claras. A especialização de cada função contribui para decisões fundamentadas e permite que o resultado seja compreendido e controlado pelas instâncias competentes.

Os apêndices seguintes oferecem uma estrutura de aplicação. Seu preenchimento deve refletir o caso, incluindo resultados negativos e hipóteses enfraquecidas. A melhor utilização desses instrumentos está em tornar o raciocínio visível, conservar a memória do trabalho e permitir revisão honesta antes da conclusão.

APÊNDICE A

Checklist de planejamento investigativo

Procedimento: _____

Responsável: _____

Data e versão do plano: _____

Delimitação e hipóteses

- ☐ Descrever o fato e separar relato de verificação.
- ☐ Definir perguntas sobre fato, autoria e circunstâncias.
- ☐ Identificar o suporte da hipótese principal.
- ☐ Formular alternativa plausível e teste correspondente.
- ☐ Prever elementos que podem contrariar a hipótese.

Fontes e medidas

- ☐ Mapear fontes, responsáveis e períodos disponíveis.
- ☐ Priorizar risco às pessoas e perda de vestígios.
- ☐ Classificar dados e fundamento de cada acesso.
- ☐ Distinguir preservação, fornecimento e exame.
- ☐ Verificar competência e autorização judicial cabível.
- ☐ Delimitar objeto, intervalo e proteção de terceiros.

Execução e revisão

- ☐ Definir executores, prazos e dependências.
- ☐ Individualizar itens e registrar sua proveniência.
- ☐ Planejar custódia, segurança e interface pericial.
- ☐ Registrar respostas parciais e resultados negativos.
- ☐ Rever hipóteses e justificar alterações do plano.
- ☐ Conferir o suporte e os limites de cada conclusão.

Pendência prioritária: _____

Decisão e responsável: _____

Instrumento didático autoral. Utilizar em conjunto com as competências, autorizações e normas institucionais aplicáveis.

APÊNDICE B

Matriz de hipóteses investigativas

Procedimento: _____

Pergunta central: _____

Data e versão: _____

Campo de controle	H1	H2	H3
Explicação proposta	_____	_____	_____
Suporte e item de origem	_____	_____	_____
Resultado esperado	_____	_____	_____
Elemento contrário possível	_____	_____	_____
Diligência para distinguir	_____	_____	_____
Fundamento e autorização	_____	_____	_____
Responsável e prazo	_____	_____	_____
Resultado e revisão	_____	_____	_____

Como preencher

Descreva hipóteses diferentes e plausíveis. No suporte, cite o identificador do elemento, sem confundir alegação com fato. No resultado esperado, indique o que a diligência poderia revelar se a hipótese estivesse correta. O elemento contrário deve ser capaz de enfraquecê-la, em aplicação do Controle de Viés Investigativo (Jorge, 2027).

Registre o resultado real e justifique a revisão. Use “não testada”, “fortalecida”, “enfraquecida” ou “permanece em aberto” como descrições de trabalho. Essas

expressões não constituem escala estatística nem padrão jurídico de suficiência para indiciamento.

Proposta autoral de aplicação do método. Amplie a matriz em folha adicional quando o caso exigir, mantendo as versões anteriores identificadas.

APÊNDICE C

Modelo de linha do tempo

Procedimento: _____

Referência temporal adotada: _____

Período e responsável: _____

Horário na fonte	Evento e item	Referência temporal	Limite ou observação
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Regras de preenchimento

Mantenha o valor registrado na fonte. Informe fuso, precisão conhecida e eventual diferença de relógio. Se houver normalização, documente cálculo, fundamento e incerteza. Não acrescente segundos a um registro que informa apenas minutos.

Relacione o evento ao item que o sustenta. Separe “ocorrência registrada”, “horário relatado” e “momento inferido”. Quando o evento puder ter ocorrido em uma faixa, apresente intervalo, sem fabricar um ponto exato.

A ordenação temporal não demonstra causalidade. Dois acontecimentos próximos podem ser independentes. Lacunas na linha do tempo devem permanecer visíveis, acompanhadas da informação necessária para entender por que não foram preenchidas.

Registro de transformação temporal: _____

Fonte do ajuste e limite: _____

Instrumento didático autoral. Conservar os registros originais e a documentação de cada transformação.

APÊNDICE D

Registro de fonte e revisão da conclusão

Procedimento e item: _____

Descrição do material: _____

Fonte de origem: _____

Canal e responsável pelo recebimento: _____

Data, hora e referência temporal: _____

Fundamento e alcance do acesso: _____

Formato e localização de guarda: _____

Transformações ou derivados: _____

Verificação de integridade aplicável: _____

Limitações de origem e completude: _____

Conferência da proposição

Afirmação que o elemento sustenta: _____

Passo de raciocínio e corroboração: _____

Hipótese alternativa testada e resultado: _____

O que o elemento não permite concluir: _____

Revisor, data e pendências: _____

Este roteiro apoia a organização investigativa. Não substitui autos, termos, laudos ou registros formais de cadeia de custódia exigidos pelo CPP e pelos protocolos institucionais.

Referências

AYERS, Richard; BROTHERS, Sam; JANSEN, Wayne. **Guidelines on mobile device forensics**. Gaithersburg: National Institute of Standards and Technology, 2014. (NIST SP 800-101, rev. 1). DOI: 10.6028/NIST.SP.800-101r1. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>. Acesso em: 18 out. 2026.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Diário Oficial da União, Brasília, DF, 5 out. 1988. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 jun. 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 13 out. 1941. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 22 jun. 2026.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, 25 jul. 1996. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19296.htm. Acesso em: 8 jul. 2026.

BRASIL. Lei nº 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Diário Oficial da União: seção 1, Brasília, DF, 21 jun. 2013. Texto disponível no portal do Senado Federal. Disponível em: <https://legis.senado.leg.br/norma/591278/publicacao/15636365>. Acesso em: 11 ago. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 5 set. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Texto consolidado. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 5 jun. 2026.

DURAND, Alain et al. **Logging recommendations for Internet-facing servers**. [S. l.]: Internet Engineering Task Force, 2011. (RFC 6302; BCP 162). Disponível em: <https://www.rfc-editor.org/rfc/rfc6302.html>. Acesso em: 15 jul. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais**. 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

KENT, Karen et al. **Guide to integrating forensic techniques into incident response**. Gaithersburg: National Institute of Standards and Technology, 2006. (NIST SP 800-86). DOI: 10.6028/NIST.SP.800-86. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. Acesso em: 21 set. 2026.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne oito cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

- Vol. 01** **Investigação Criminal Tecnológica.** Fundamentos, métodos e aplicações práticas (este volume)
- Vol. 02** **Provas digitais e cadeia de custódia.** Da coleta à valoração jurídica
- Vol. 03** **Inteligência artificial na investigação criminal.** Aplicações, limites e boas práticas
- Vol. 04** **Golpes digitais e fraudes eletrônicas.** Prevenção, identificação e investigação
- Vol. 05** **Investigação de crimes na internet.** Dados, registros, sigilos e medidas judiciais
- Vol. 06** **Raciocínio investigativo e decisão fundamentada.** Do indício ao relatório final
- Vol. 07** **Internet segura.** Guia prático para proteger você e sua família
- Vol. 08** **Crianças e adolescentes na internet.** Guia de proteção para pais e responsáveis

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge